 DCI / IA

U.S. Department of Justice

Office of the Deputy Attorney General



The Deputy Attorney General

Washington, D.C. 20530

26 JAN 1984



MEMORANDUM FOR THOSE ATTENDING 4:30 MEETING ON JANUARY 27, 1984

## Introduction

President Reagan signed National Security Decision Directive 84 (NSDD-84) on March 11, 1983. (See Tab A.) This directive contains a number of measures to safeguard classified information from unauthorized disclosure. Implementation of the directive has been delayed by controversy regarding two aspects.

-- Paragraph 1.b. of the directive requires that persons with access to Sensitive Compartmented Information (SCI) sign secrecy agreements that include a pre-publication review provision. This sort of "lifetime censorship agreement" has been upheld by the Supreme Court in the Snepp case and used at CIA and NSA for some years. (See Tab B.)

-- Paragraph 5 of the directive requires that agencies clarify their policies so that "appropriate adverse consequences" could follow an employee's refusal to be polygraphed in a leak investigation. This does not require use of the polygraph in any particular case; it does mean that agency policies cannot effectively preclude polygraph use. (See Tab C.)

This controversy has become linked to an unrelated Department of Defense proposal to permit greater use of the polygraph in determining security clearances for certain employees in highly sensitive jobs. (See Tab C.) In addition, some press critics have linked these measures with other Administration initiatives as part of an overall program to squelch the First Amendment. (See Tab D.)

## Issue for Decision

Congress has enacted legislation that blocks -- until April 15, 1984 -- any change in polygraph policy at the Department of Defense, and any new policy regarding prepublication review throughout the government. It is quite likely that legislation will be introduced to extend the current moratoria until 1985 or to impose permanent restrictions on the use of polygraphs and prepublication review.

We need to decide how to respond to this legislative challenge. Administration witnesses will be called to testify starting on February 7 before a joint hearing of subcommittees chaired by Don Edwards and Pat Schroeder. Senator Mathias also plans hearings in February. Other hearings are likely.

## Options

(1) Abandon efforts to implement these controversial policies, at least prior to 1985. A public announcement to this effect would probably eliminate most of the congressional hearings and deprive the issue of immediate significance. Permanent legislation could be avoided and, at most, the current moratoria would be extended another year.

Implementation of this option would require revocation or suspension of paragraphs 1.b. and 5 of NSDD-84. This could be combined with option 3 so as to avoid an impression that we no longer care about this problem.

(2) Seek to implement these policies, with some modifications, and oppose further legislative restrictions. The intelligence committees, especially in the Senate, are likely to be most sympathetic to these policies. However, some modifications (at least in the prepublication review program) will be necessary to win sufficient support. The precise modifications would have to be developed in consultation with key Senators (such as Chafee, Lugar, and Huddleston).

For example, the prepublication review agreement could be modified to require submissions for a limited period of time (e.g., 12 years) after leaving the government. Another possible change would be to limit the scope of materials required to be submitted for review. Such modifications would not require any change in NSDD-84 itself, only in the manner of implementation.

Successful pursuit of this option will require indications from the White House to key Senators that the Administration is serious about implementing these policies, as modified. The White House legislative affairs and communications office would have to work closely with NSC, Justice, CIA and Defense in this

effort. It would be particularly helpful if CIA and NSA could declassify a few specific examples of the damage to national security caused by unauthorized disclosures of classified information.

(3) Seek to enact new legislation to address the problem. The intelligence community has long sought a comprehensive criminal statute to punish unauthorized disclosures of classified information. A statute providing civil penalties could be sought instead of, or in addition to, a criminal statute. Enactment of such legislation would provide more effective remedies than are available under existing law and administrative regulations.

The chances of getting such legislation enacted this year are practically nonexistent. The main purpose of this option is to begin a long-range campaign for enactment in 1985 or later.

Edward C. Schmults
Deputy Attorney General

Tab A: General Reference

Text of NSDD-84, Mar. 11, 1983
President's Memorandum for Federal Employees
Statistics on August 30, 1983 Security Clearances and Classification Activity

Tab B: Prepublication Review

Development of Policy
Some Fiction and Facts about Prepublication Review
Form 4193 (Dec. 1981)
New SCI Nondisclosure Agreement (Aug. 1983)

Tab C: Polygraphs

Four Categories of Polygraph Use
Use of Polygraph in Leak Investigations
DOD Polygraph Screening Proposal
Statistics on Federal Polygraph Use
Statistics on Polygraph Accuracy

Tab D: Related Issues of Legislative Interest

Proposals to Amend FOIA
Executive Order on Classification (E.O. 12356)
New FBI Domestic Security/Terrorism Guidelines

## Safeguarding National Security Information

As stated in Executive Order 12356, only that information whose disclosure would harm the national security interests of the United States may be classified. Every effort should be made to declassify information that no longer requires protection in the interest of national security.

At the same time, however, safeguarding against unlawful disclosures of properly classified information is a matter of grave concern and high priority for this Administration. In addition to the requirements set forth in Executive Order 12356, and based on the recommendations contained in the interdepartmental report forwarded by the Attorney General, I direct the following:

1. Each agency of the Executive Branch that originates or handles classified information shall adopt internal procedures to safeguard against unlawful disclosures of classified information. Such procedures shall at a minimum provide as follows:

a. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. This requirement may be implemented prospectively by agencies for which the administrative burden of compliance would otherwise be excessive.

b. All persons with authorized access to Sensitive Compartmented Information (SCI) shall be required to sign a nondisclosure agreement as a condition of access to SCI and other classified information. All such agreements must include a provision for prepublication review to assure deletion of SCI and other classified information.

c. All agreements required in paragraphs 1.a. and 1.b. must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States. The Director, Information Security Oversight Office (ISOO), shall develop standardized forms that satisfy these requirements.

d. Appropriate policies shall be adopted to govern contacts between media representatives and agency personnel, so as to reduce the opportunity for negligent or deliberate disclosures of classified information. All persons with authorized access to classified information shall be clearly apprised of the agency's policies in this regard.

2. Each agency of the Executive branch that originates or handles classified information shall adopt internal procedures to govern the reporting and investigation of unauthorized disclosures of such information. Such procedures shall at a minimum provide that:

a. All such disclosures that the agency considers to be seriously damaging to its mission and responsibilities shall be evaluated to ascertain the nature of the information disclosed and the extent to which it had been disseminated.

b. The agency shall conduct a preliminary internal investigation prior to or concurrently with seeking investigative assistance from other agencies.

c. The agency shall maintain records of disclosures so evaluated and investigated.

d. Agencies in the possession of classified information originating with another agency shall cooperate with the originating agency by conducting internal investigations of the unauthorized disclosure of such information.

e. Persons determined by the agency to have knowingly made such disclosures or to have refused cooperation with investigations of such unauthorized disclosures will be denied further access to classified information and subjected to other administrative sanctions as appropriate.

3. Unauthorized disclosures of classified information shall be reported to the Department of Justice and the Information Security Oversight Office, as required by statute and Executive orders. The Department of Justice shall continue to review reported unauthorized disclosures of classified information to determine whether FBI investigation is warranted. Interested departments and agencies shall be consulted in developing criteria for evaluating such matters and in determining which cases should receive investigative priority. The FBI is authorized to investigate such matters as constitute potential violations of federal criminal law, even though administrative sanctions may be sought instead of criminal prosecution.

4. Nothing in this directive is intended to modify or preclude interagency agreements between FBI and other criminal investigative agencies regarding their responsibility for conducting investigations within their own agencies or departments.

5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies, as necessary, so that employees may be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information. As a minimum, such regulations shall permit an agency to decide that appropriate

adverse consequences will follow an employee's refusal to cooperate with a polygraph examination that is limited in scope to the circumstances of the unauthorized disclosure under investigation. Agency regulations may provide that only the head of the agency, or his delegate, is empowered to order an employee to submit to a polygraph examination. Results of polygraph examinations should not be relied upon to the exclusion of other information obtained during investigations.

6. The Attorney General, in consultation with the Director, Office of Personnel Management, is requested to establish an interdepartmental group to study the federal personnel security program and recommend appropriate revisions in existing Executive orders, regulations, and guidelines.

Exhibit A

THE WHITE HOUSE

WASHINGTON

August 30, 1983

SEP 9 4 21 PM '83

MEMORANDUM FOR FEDERAL EMPLOYEES

SUBJECT: Unauthorized Disclosure of Classified Information

Recent unauthorized disclosures of classified information concerning our diplomatic, military, and intelligence activities threaten our ability to carry out national security policy. I have issued a directive detailing procedures to curb these disclosures and to streamline procedures for investigating them. However, unauthorized disclosures are so harmful to our national security that I wish to underscore to each of you the seriousness with which I view them.

The unauthorized disclosure of our Nation's classified information by those entrusted with its protection is improper, unethical, and plain wrong. This kind of unauthorized disclosure is more than a so-called "leak"--it is illegal. The Attorney General has been asked to investigate a number of recent disclosures of classified information. Let me make it clear that we intend to take appropriate administrative action against any Federal employee found to have engaged in unauthorized disclosure of classified information, regardless of rank or position. Where circumstances warrant, cases will also be referred for criminal prosecution.

The American people have placed a special trust and confidence in each of us to protect their property with which we are entrusted, including classified information. They expect us to protect fully the national security secrets used to protect them in a dangerous and difficult world. All of us have taken an oath faithfully to discharge our duties as public servants, an oath that is violated when unauthorized disclosures of classified information are made.

Secrecy in national security matters is a necessity in this world. Each of us, as we carry out our individual duties, recognizes that certain matters require confidentiality. We must be able to carry out diplomacy with friends and foes on a confidential basis; peace often quite literally depends on it--and this includes our efforts to reduce the threat of nuclear war.

We must also be able to protect our military forces from present or potential adversaries. From the time of the Founding Fathers, we have accepted the need to protect military secrets. Nuclear dangers, terrorism, and aggression similarly demand

that we must be able to gather intelligence information about these dangers--and our sources of this information must be protected if we are to continue to receive it. Even in peacetime, lives depend on our ability to keep certain matters secret.

As public servants, we have no legitimate excuse for resorting to these unauthorized disclosures. There are other means available to express ourselves:

-- We make every effort to keep the Congress and the people informed about national security policies and actions. Only a fraction of information concerning national security policy must be classified.

-- We have mechanisms for presenting alternative views and opinions within our government.

-- Established procedures exist for declassifying material and for downgrading information that may be overclassified.

-- Workable procedures also exist for reporting wrongdoing or illegalities, both to the appropriate Executive Branch offices and to the Congress.

Finally, each of us has the right to leave our position of trust and criticize our government and its policies, if that is what our conscience dictates. What we do not have is the right to damage our country by giving away its necessary secrets.

We are as a Nation an open and trusting people, with a proud tradition of free speech, robust debate, and the right to disagree strongly over all national policies. No one would ever want to change that. But we are also a mature and disciplined people who understand the need for responsible action. As servants of the people, we in the Federal Government must understand the duty we have to those who place their trust in us. I ask each of you to join me in redoubling our efforts to protect that trust.

Ronald Reagan

## Statistics on Security Clearances and Classification Activity

### Security Clearances (Excluding CIA and NSA)

| | Employees | Contractors |
|---|---|---|
| Top Secret - SCI | 112,000 | 15,000 |
| Top Secret - No SCI | 351,000 | 252,000 |
| Secret | 2,055,000 | 940,000 |
| Confidential | 17,000 | 305,000 |
| Total Clearances | 2,535,000 | 1,512,000 |

### Changes in Classification Activity

| | Original Classification | Original Plus Derivative Classification |
|---|---|---|
| FY 80 (Carter) | about same | up 10% |
| FY 81 (transition) | about same | up 8% |
| FY 82 (Reagan) | about same | up 1% |
| FY 83 (Reagan) | down 18% | up 3% |

B

## Prepublication Review: Development of Policy

For many years CIA employees have signed secrecy agreements requiring them to obtain agency clearance before publishing materials that might contain classified information. A number of court decisions have upheld the enforceability of these agreements, including the Supreme Court's decision in Snepp v. United States (1980).

Civiletti Guidelines. In December 1980, shortly before leaving office, Attorney General Civiletti adopted guidelines to limit the discretion of the Justice Department in enforcing contractual secrecy obligations. These guidelines in effect overruled some of the broader implications of the Supreme Court's opinion in the Snepp case.

Guideline Revocation. In September 1981, Attorney General Smith revoked the Civiletti guidelines because they suggested the United States would not enforce secrecy obligations to the extent permitted by the Snepp decision. The new policy is to "evenhandedly and strenuously" enforce secrecy obligations. The personal approval of the Attorney General is required before initiating any such litigation.

Form 4193. In 1981, DCI Casey promulgated a new secrecy agreement (Form 4193) for all government employees with access to SCI, which contains a prepublication review provision. This agreement was initially drafted during the Carter Administration as part of a broader plan to upgrade information security standards (APEX) which was ultimately abandoned. The language of this agreement has several defects that would make it difficult to enforce. For example, it only authorized deletion of SCI (not Secret or Top Secret information) from manuscripts that are submitted for prepublication review.

NSDD-84. This directive was issued by the President in March 1983. It requires two new standard secrecy agreements, to be approved by the Justice Department as enforceable in civil litigation. The two agreements were developed by an interdepartmental committee under supervision of the NSC staff, approved by the Justice Department, and publicly announced in August 1983.

-- The classified information nondisclosure agreement does not include a provision for prepublication review and has not been very controversial. However, many agencies have refused to implement this agreement because of controversy regarding the SCI nondisclosure agreement.

-- The SCI nondisclosure agreement replaces Form 4193 and includes a prepublication review provision. Because the Mathias amendment (discussed below) was introduced soon after its promulgation, very few officials have signed the new agreement.

The Mathias Amendment. On October 20, 1983, the Senate adopted by a vote of 56-34 this amendment to the State Department authorization bill, which was finally enacted on November 22. The amendment prohibits until April 15, 1984, any prepublication review agreement or policy that was not in effect prior to March 1983. The stated purpose is to delay implementation of the new SCI nondisclosure agreement so that Congress has time to study the issue further. The Mathias amendment does not interfere with the continued use and enforcement of Form 4193.

House Committee Report. On November 22, 1983, a majority of the House Government Operations Committee approved a report recommending appropriate legislation unless the President rescinds the portion of NSDD-84 requiring prepublication review agreements. Six Republicans signed a dissenting statement supporting the President's directive, but recommending that consideration be given to replacing the lifetime prepublication review provision with a commitment limited to a reasonable period of time after leaving government employment.

Congressional Outlook. There is little congressional interest in preventing CIA and NSA from continuing their prepublication review programs. However, there is substantial opposition to requiring prepublication review for other employees with SCI access. This opposition applies to both the new nondisclosure agreement as well as the old Form 4193 (which went unnoticed when originally promulgated).

## Some Fiction and Facts About Prepublication Review

**Fiction:** Secrecy agreements requiring prepublication review violate the First Amendment.

**Fact:** The Supreme Court upheld the constitutionality of prepublication review for CIA employees in Snepp v. United States (1980).

* * * *

**Fiction:** The Reagan Administration wants to extend prepublication review to millions of government employees with access to classified information.

**Fact:** The requirement will only apply to employees with access to Sensitive Compartmented Information (SCI). There are about 112,000 such employees, most in the Department of Defense, who were not previously covered.

* * * *

**Fiction:** Employees covered by this agreement will have to submit for review anything they ever write for the rest of their lives.

**Fact:** Only materials that include information relating to specified intelligence matters will have to be submitted.

* * * *

**Fiction:** This program will allow the Administration in power to censor views of people they disagree with.

**Fact:** Only classified information can be deleted. Judicial review is provided, and the government must be able to prove in court that every word it wants to delete is properly classified.

* * * *

Fiction: Prepublication review will keep authors from publishing their views in a timely manner.

Fact: The agreement requires review to be conducted in 30 days as a maximum. Last year, CIA conducted 213 such reviews and completed them in an average of 13 days. Reviews have been conducted in a matter of hours for authors working on short deadlines.

* * * *

Fiction: This program will effectively prevent former officials from giving speeches, press interviews or appearing on talk shows, because they cannot submit their answers for review in advance.

Fact: Prepublication review does not apply to extemporaneous oral comments. Only if oral statements are given from a prepared text is there a requirement to submit for review.

* * * *

Fiction: This program is unnecessary because former employees hardly ever disclose classified information in books or speeches.

Fact: Since 1977, some 929 items have been submitted to CIA for prepublication review, of which 241 contained classified information that was protected by the program. A similar opportunity to protect classified information would exist for other employees with access to equally sensitive information.

* * * *

# SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement Between _____ and the United States
(Name – Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or classifiable under the standards of Executive Order 12065 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge such information to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I further understand that I am obligated by law and regulation not to disclose any classified information in an unauthorized fashion.

4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information, all information or materials, including works of fiction, which contain or purport to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such information and materials for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the information or materials with, or showing them to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose such information or materials to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.

5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the information or materials submitted pursuant to paragraph 4 set forth any SCI. I further understand that the Department or Agency to which I have submitted materials will act upon them, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.

6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and retention in a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys fees incurred by the United States Government may be assessed against me if I lose such action.

8. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials, which may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12065, as amended, so that I may read them at this time, if I so choose.

12. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. I make this Agreement

SIGNATURE _____ DATE _____

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE:

SIGNATURE _____ DATE _____

## SECURITY BRIEFING ACKNOWLEDGMENT

I hereby acknowledge that I was briefed on the following SCI Special Access Program(s):

(Special Access Programs by Initials Only)

Signature of Individual Briefed _____ Date Briefed _____

Printed or Typed Name _____

Social Security Number (See Notice Below) _____ Organization (Name and Address) _____

I certify that the above SCI access(es) were approved in accordance with relevant SCI procedures and that the briefing presented by me on the above date was also in accordance therewith.

Signature of Briefing Officer _____

Printed or Typed Name _____ Organization (Name and Address) _____

Social Security Number (See Notice Below) _____

* * * * *

## SECURITY DEBRIEFING ACKNOWLEDGMENT

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the following SCI Special Access Program(s):

(Special Access Programs by Initials Only)

Signature of Individual Debriefed _____ Date Debriefed _____

Printed or Typed Name _____

Social Security Number (See Notice Below) _____ Organization (Name and Address) _____

I certify that the debriefing presented by me on the above date was in accordance with relevant SCI procedures.

Signature of Debriefing Officer _____

Printed or Typed Name _____ Organization (Name and Address) _____

Social Security Number (See Notice Below) _____

NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.

Exhibit C

# Sensitive Compartmented Information Nondisclosure Agreement

An Agreement between _____ and the United States
(Name—Printed or Typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information known as Sensitive Compartmented Information (SCI). I have been advised and am aware that SCI involves or derives from intelligence sources or methods and is classified or classifiable under the standards of Executive Order 12356 or under other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures. I understand that I may be required to sign subsequent agreements as a condition of being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.

3. I have been advised and am aware that direct or indirect unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me either a security clearance or an SCI access approval that such disclosure is permitted.

4. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information. As used in this Agreement, classified information is information that is classified under the standards of E.O. 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security.

5. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI and other classified information, I hereby agree to submit for security review by the Department or Agency last granting me either a security clearance or an SCI access approval all materials, including works of fiction, that I contemplate disclosing to any person not authorized to have such information, or that I have prepared for public disclosure, which contain or purport to contain:

(a) any SCI, any description of activities that produce or relate to SCI, or any information derived from SCI;
(b) any classified information from intelligence reports or estimates; or
(c) any information concerning intelligence activities, sources or methods.

I understand and agree that my obligation to submit such information and materials for review applies during the course of my access to SCI and at all times thereafter. However, I am not required to submit for review any such materials that exclusively contain information lawfully obtained by me at a time when I have no employment, contract or other relationship with the United States Government, and which are to be published at such time.

6. I agree to make the submissions described in paragraph 5 prior to discussing the information or materials with, or showing them to anyone who is not authorized to have access to such information. I further agree that I will not disclose such information or materials unless I have officially verified that the recipient has been properly authorized by the United States Government to receive it or I have been given written authorization from the Department or Agency last granting me either a security clearance or an SCI access approval that such disclosure is permitted.

7. I understand that the purpose of the review described in paragraph 5 is to give the United States a reasonable opportunity to determine whether the information or materials submitted pursuant to paragraph 5 set forth any SCI or other information that is subject to classification under E. O. 12356 or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security. I further understand that the Department or Agency to which I have submitted materials will act upon them coordinating with the Intelligence Community or other agencies when appropriate, and substantively respond to me within 30 working days from date of receipt.

8. I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances and SCI access approvals that I may hold; removal from any position of special confidence and trust requiring such clearances or access approvals; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearances or SCI access approvals. In addition, I have been advised and am aware that any unauthorized disclosure of SCI or other classified information by me may constitute a violation or violations of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and 952, Title 18, United States Code, the provisions of Section 783 (b), Title 50, United States Code and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

9. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

10. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

11. I understand that all information to which I may obtain access by signing this Agreement is now and will forever remain the property of the United States Government. I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to this information. I agree that I shall return all materials which have or may come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the Department or Agency that last granted me either a security clearance or an SCI access approval. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

12. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI and at all times thereafter.

13. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

14. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, Section 783 (b) of Title 50, United States Code, the Intelligence Identities Protection Act of 1982, and Executive Order 12356 so that I may read them at this time, if I so choose.

15. I make this Agreement without mental reservation or purpose of evasion.

Signature _____ Date _____

Social Security Number (see notice below) _____ Organization _____

The execution of this Agreement was witnessed by the undersigned, who, on behalf of the United States Government, agreed to its terms and accepted it as a prior condition of authorizing access to *Sensitive Compartmented Information*.

WITNESS and ACCEPTANCE:

Signature _____ Date _____

Organization _____

Notice: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information indicated has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations.

## Four Categories of Polygraph Use

There are two basic ways to use the polygraph: for screening and in particular investigations. Screening examinations are not designed to solve specific cases of suspected misconduct, but instead are preventive in nature. Questions in a screening examination are to determine whether an individual meets security standards for employment or access to classified information.

(1) Polygraph Screening as a Condition of Employment.--

-- CIA and NSA have used the polygraph as part of their security screening program for many years, both prior to employment and periodically thereafter.

(2) Polygraph Screening as a Condition of Access to Information.--

-- In 1982, DOD proposed a new polygraph screening program for certain employees with access to highly classified information.

In addition to its use for screening, the polygraph is also used as a technique to investigate particular cases of suspected wrongdoing, including unauthorized disclosures of classified information.

(3) Criminal Investigations.--

-- In a criminal investigation, the Fifth Amendment requires a subject to consent to the polygraph. Because of undue influence on the jury and for other reasons, DOJ routinely opposes introduction of polygraph evidence in criminal trials. However, DOJ supports its use as an investigative technique. (Hearsay may also be inadmissible evidence but is relied upon in investigations.)

(4) Administrative Investigations.--

-- In administrative investigations, the Fifth Amendment does not preclude the government from requesting or requiring employees to be polygraphed. The polygraph has been used in such investigations for some years. (For example, Attorney General Civiletti approved use of the polygraph in the ABSCAM leak investigation in 1980.)

## Use of Polygraph in Leak Investigations

The polygraph has been used for a number of years in investigating unauthorized disclosures of classified information. However, there has been some uncertainty about the extent to which the government could encourage or require employees to be polygraphed in such cases. In NSDD-84 President Reagan ordered agencies to clarify their policies so that "appropriate adverse consequences" could follow an employee's refusal to be polygraphed.

Drafting of regulations to implement this aspect of NSDD-84 was initially delayed so that the Office of Legal Counsel could prepare a memorandum analyzing the impact of the MSPB's 1980 decision in the Meier case. See Memorandum of Theodore B. Olson, August 22, 1983. We have now developed specific legal and policy guidance for implementing this aspect of NSDD-84, which was contained in DOJ testimony before the House Government Operations Committee in October 1983.

-- The unauthorized disclosure must be a serious offense affecting national security or the integrity of the employee's official conduct.

-- The polygraph can only be used after investigation by other means has produced a substantial objective basis for seeking to examine a particular employee.

-- The polygraph can only be used if there is no other reasonable means to resolve the matter.

-- Questions must be limited to the circumstances of the unauthorized disclosure and cannot go into "life style" matters.

-- The examination results cannot be conclusive and must be considered in the context of all available information.

The consequences of an employee's refusal to take a polygraph examination will depend upon all the facts and circumstances.

-- Employees in the competitive service or uniformed services (the vast majority of federal employees) cannot be fired or demoted solely for refusing to be polygraphed. However, they could be transferred to a less sensitive job at the same level of pay.

-- Political appointees are subject to more rigorous standards and could be fired in an appropriate case for refusing to be polygraphed.

## DOD Polygraph Screening Proposal
(The "Random" Polygraph)

The Department of Defense announced this proposal in 1982, but it has not yet been implemented because of a congressional moratorium until April 15, 1984. Administration witnesses testified in support of this policy before the House Government Operations Committee in October 1983.

-- Only employees in "special access programs" could be covered -- a maximum of about 100,000 in DOD and about 10,000 in other agencies if the program were extended outside DOD.

-- The head of each agency has discretion to decide whether, and to what extent to use it. Only DOD has current plans to adopt this program.

-- Questions are limited to "counterintelligence" matters, such as whether the employee has disclosed classified information to a foreign agent or other unauthorized person. "Life style" questions are not permitted.

-- Employees in the competitive service and uniformed services (the vast majority of federal employees) who do not agree to be polygraphed can be transferred to less sensitive jobs. They cannot be fired or demoted.

-- Not even all of these employees will necessarily be polygraphed. A smaller number can be randomly selected for polygraphs each year. Random selection protects these employees from being singled out to be polygraphed for discriminatory reasons.

Note: This program is not primarily designed to counter "leaks." It is to safeguard sensitive classified information that is likely to be of extraordinary interest to hostile intelligence agents. It is part of an effort to upgrade security standards for employees outside of CIA and NSA who have access to the same kind of highly sensitive information.

## Statistics on Federal Polygraph Use

| | CIA | NSA | DOD (Not NSA) | Other Agencies | Total (Except CIA) |
|---|---|---|---|---|---|
| FY 80 (Carter) | NA | 5,676 | 7,374 | 3,241 | 16,291 |
| FY 81 (Transition) | NA | 7,418 | 7,007 | 3,807 | 18,232 |
| FY 82 (Reagan) | NA | 9,672 | 8,629 | 4,296 | 22,597 |

Notes: CIA and NSA examinations were nearly all for personnel screening. Over 90% of all other examinations were given in criminal investigations (suspects, witnesses, informants, victims).

In 1980-82, a total of about 260 examinations were given in cases of unauthorized disclosure of sensitive or classified information.

Source: OTA Study (Nov. 1983), p. 108.

## Statistics on Polygraph Accuracy

| | Field Studies | Laboratory Studies | |
|---|---|---|---|
| | | Control Question Technique | Guilty Knowledge Technique |
| Accurate | 82.0 | 60.9 | 80.5 |
| Inaccurate: | | | |
| False Positive | 8.2 | 6.8 | 2.2 |
| False Negative | 5.8 | 5.4 | 17.3 |
| Inconclusive | 4.1 | 26.9 | 0 |

Note: Percentages reflect mean detection rates of polygraph validity studies reported and analyzed by OTA. All involve single-issue examinations for actual or simulated criminal conduct.

Source: OTA Study (Nov. 1983), pp. 52 and 65.

D

## Freedom of Information Act Amendments

An early priority of this Administration was to seek amendments to the Freedom of Information Act. This has evolved into two tracks: general reform and relief for CIA. Each of these tracks has produced bills with wide bipartisan support in the Senate but uncertain prospects in the House.

S.774. This is the general FOIA reform bill, which is supported by Senators Hatch and Leahy. It was unanimously approved by the Senate Judiciary Committee in June 1983 and is awaiting action by the full Senate. Among other things, this bill would improve the protection of law enforcement information in government files.

S. 1324. This is the CIA relief bill. CIA originally sought total exemption from FOIA but earlier this year sought a compromise. S. 1324 is the result. It exempts CIA operational files, which are unlikely to contain any information that is releasable, from the budensome requirement of FOIA searches. However, all other CIA files remain fully subject to FOIA. S. 1324 was unanimously approved in October 1983 by the Senate Intelligence Committee with strong bipartisan support, and by the full Senate in November of 1983.

Congressional Outlook--It is expected that the full Senate will approve S. 774 in the next few weeks. It will then be referred to the Subcommittee on Government Information of the House Government Operations Committee, chaired by Congressman Glenn English (D-Okla.). While it is expected that English will hold hearings, he generally opposes FOIA reform and House action is unlikely.

Prospects for S. 1324 are considerably better however. The bill has been referred jointly to the House Intelligence Committee, which has scheduled a hearing for February 8, and the Government Operations Committee. Although Congressman English could block this legislation as well, it has fairly strong support in the House and a fair chance of passage.

## Executive Order 12356 (Classified Information)

President Reagan signed Executive Order 12356, "National Security Information" on April 2, 1982. The new Order includes a number of changes that are based on litigative and administrative experience under its predecessor order, which was issued by President Carter in 1978. These changes are designed to enhance the Executive branch's ability to protect national security information from unauthorized disclosure and are not intended to increase the quantity of classified information.

The two most controversial changes are:

-- The minimum standard for classification requires a determination that unauthorized disclosure "reasonably could be expected to cause damage to the national security." The Carter order required "identifiable damage."

-- The Reagan order eliminates the "balancing test," in which classifying officials were required to balance the public interest in disclosure against the need for secrecy.

Both of these changes were made to avoid problems in protecting classified information in litigation, primarily under FOIA.

Statistics recently compiled by the Information Security Oversight Office (ISOO) show that the new order has not produced an increase in the amount of classified information. During the first year that the new order was in effect (FY 1983), original classification activity declined by 18%, which was the first significant decline in four years. Total classification activity (including derivative classification) increased by only 3%, which is much lower than the 8-10% annual increases during the last two years of the Carter Administration.

Congressional Outlook.--Legislation has been introduced in the House and Senate to provide statutory standards for classification. If enacted, this legislation would effectively repeal the Reagan order and replace it with the Carter order. Hearings have been held on the general subject, but passage of legislation seems unlikely.

## FBI Domestic Security/Terrorism Guidelines

The new Domestic Security/Terrorism Guidelines became effective March 21, 1983, replacing guidelines previously issued by Attorney General Levi in 1976 (the "Levi Guidelines").

The new guidelines incorporate instructions for domestic security cases in the existing General Crimes and Racketeering Enterprise Guidelines, thus giving the FBI a single set of procedures for all criminal and criminal intelligence investigations. This provides a consistency which did not exist in the past. In addition, the guidelines:

-- Eliminate the three-tiered approach to domestic security cases,

-- Use a criminal enterprise approach which emphasizes the intelligence nature of these cases,

-- Encourage the continued monitoring of criminal enterprises even when they may be temporarily inactive,

-- Make clear that the FBI may take into account statements made by enterprise members which indicate an apparent intent to engage in crime.

On April 18, 1983, Judge Getzendanner of the Northern District of Illinois permanently enjoined in the City of Chicago the provision of the guidelines permitting the FBI to initiate inquiries or investigations on the basis of statements advocating criminal conduct. Alliance to End Repression v. City of Chicago, No. 74C3268. The government is appealing this ruling. The court denied preliminary injunctions directed to certain other sections of the guidelines.

Congressional Outlook.--Congressman Don Edwards has introduced legislation that would block implementation of the new guidelines, with the apparent intent of requiring a return to the Levi Guidelines. Hearings have been held on the new guidelines, but passage of blocking legislation seems unlikely.